This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS:

A1

Claim 1 (Currently Amended): A system for controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said system comprising:

means for determining fulfillment of one or more certain conditions at said destination location, said means including means enabling a sender of a communicated package to observe a user requesting access to content at said destination location, said condition including sender identification of said user; and,

control means responsive to detection of a fulfilled one or more certain conditions for enabling access to content provided in a communicated package, whereby said access includes enabling a user to perform an operation on said package content at said destination location.

Claim 2 (Original): The system as claimed in Claim 1, wherein said electronic information packages include content comprising one or more of: e-mail messages, audio data, video data, animation data, textual data, and pictorial data.

Claim 3 (Original): The system as claimed in Claim 2, further including means for automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions.

A1

Claim 4 (Original): The system as claimed in Claim 3, wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals, said system further comprising means for determining elapsed time from receipt of an electronic information package, said means generating a signal for destroying the received electronic information package after a time interval has elapsed.

Claim 5 (Original): The system as claimed in Claim 4, wherein said elapsed time interval is specified by a sender at said sending device, said electronic information package further comprising a specification of one or more time-out intervals for use by said elapsed timing means.

Claim 6 (Original): The system as claimed in Claim 5, wherein said operations enabled to be performed on said package content at said destination device include displaying one or more of video data, text, picture and animation data via a display device at said destination location.

Claim 7 (Original): The system as claimed in Claim 5, wherein said operations enabled to be performed on said package content at said destination device include playing audio data on one or several speakers at said destination location.

Claim 8 (Original): The system as claimed in Claim 3, wherein said access includes forbidding a user to perform an operation on said package content at said destination device, said operations that are forbidden to be performed on received information packages include one or more of:

A1

saving, copying and downloading the received information package content in a memory storage device and printing said package content at said at a destination location.

Claim 9 (Original): The system as claimed in Claim 8, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting an attempted performance of a forbidden operation at the destination location, said destroying means automatically destroying a received electronic information package in response to said detection.

Claim 10 (Original): The system as claimed in Claim 8, wherein said means for determining fulfillment of one or more certain conditions at said destination device further includes means for receiving a direct command signal from a sender at a sending device, said sender command triggering destruction of said electronic information package.

Claim 11 (Original): The system as claimed in Claim 8, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, said physical hardware devices including CPU, memory or peripherals at said destination device, said destroying means automatically destroying a received electronic information package in response to said detection.

Claim 12 (Original): The system as claimed in Claim 8, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means

A1

for detecting a second or repeated attempted to play or display information package content, said destroying means automatically destroying a received electronic information package in response to said detection.

Claim 13 (Original): The system as claimed in Claim 9, wherein said means for detecting an attempted performance of a forbidden operation at the destination location, includes means operable in conjunction with an operating system at said destination device, for detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying, downloading, printing, and saving, received electronic information packages.

Claim 14 (Original): The system as claimed in Claim 9, wherein said means for detecting an attempted performance of a forbidden operation at the destination location, includes means operable in conjunction with an operating system at said destination device, for detecting a pressing of a key on a keyboard operable for said destination device.

Claim 15 (Original): The system as claimed in Claim 1, wherein said means for determining fulfillment of one or more certain conditions at said destination location includes identification means for identifying a user at said destination location for which access to these information packages is allowed.

Claim 16 (Currently Amended): The system as claimed in Claim ~~15~~ 1, wherein said ~~identification~~ means enabling a sender of a communicated package to observe a user requesting

A1

access to content includes video camera system for generating video signals at said destination device and a display device for receiving and displaying video signals at said sending device, said video camera system enabling a sender at a sending device to observe users attempting to read or play information package content at a destination device.

Claim 17 (Original): The system as claimed in claim 15, wherein said identification means for identifying a user at said destination location comprises:

means for enabling users to present a password to said system; and,

verification means for verifying a user's password prior to enabling access to said information package.

Claim 18 (Original): The system as claimed in Claim 15, wherein said identification means for identifying a user at said destination location comprises means for enabling users to present a data for authentification/verification that include one or more of the following: biometrics, fingerprint, and voice data.

Claim 19 (Original): The system as claimed in Claim 1, wherein said means for determining fulfillment of one or more certain conditions at said destination location includes identification means for identifying an electronic system at said destination location for which access to these information packages is allowed.

Claim 20 (Original): The system as claimed in Claim 19, wherein said electronic system trying to access information packages comprises a communication process that supports transferring electronic package content via a communication channel to new destination locations.

Claim 21 (Original): The system as claimed in Claim 19, wherein said electronic system trying to access information packages comprises an automated process capable of understanding information package content and performing necessary operations as required for playing said content.

Claim 22 (Original): The system as claimed in Claim 19, wherein said electronic system trying to access information packages comprises a robotic device.

Claim 23 (Original): The system as claimed in Claim 1, wherein said electronic information packages communicated from a sending device to a device at one or more destination locations, is communicated over a communications channel including one or more of: telephone wires, wireless channels, radio links, network data connection.

Claim 24 (Currently Amended): A method for controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said method comprising:

determining fulfillment of one or more conditions at said destination location, said determining including enabling a sender of a communicated package to observe a user requesting access to content at said destination location and identify said user as a condition; and,

A1

in response to determination of a fulfilled one or more certain conditions, enabling access to content provided in a communicated package.

Claim 25 (Original): The method as claimed in Claim 24, further including the step of automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions.

Claim 26 (Original): The method as claimed in Claim 25, wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals from receipt of an electronic package, said method further comprising the steps of:

determining elapsed time from receipt of an electronic information package; and,

generating a signal for initiating automatic destruction of the received electronic information package after said elapsed time interval.

Claim 27 (Original): The method as claimed in Claim 26, further including the step of enabling a sender to specify said time interval.

Claim 28 (Original): The method as claimed in Claim 24, wherein said step of enabling access to said content of said communicated package includes enabling a user to display one or more of video data, text, picture and animation data via a display device at said destination location, and play audio data on one or several speakers at said destination location.

A1

Claim 29 (Original): The method as claimed in Claim 28, wherein said step of enabling access to said content of said communicated package includes forbidding a user to perform an operation on said package content at said destination device, said operations forbidden to be performed on received information packages including one or more of: saving, copying and downloading the received information package content in a memory storage device and printing said package content at said at a destination location.

Claim 30 (Original): The method as claimed in Claim 28, wherein said enabling step of determining fulfillment of one or more conditions at said destination device further comprises detecting an attempted performance of a forbidden operation at the destination location; and, in response to said detecting, automatically destroying a received electronic information package.

Claim 31 (Original): The method as claimed in Claim 28, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: receiving a direct command signal from a sender at a sending device for initiating destruction of said electronic information package.

Claim 32 (Original): The method as claimed in Claim 28, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, said physical hardware devices including CPU, memory or peripherals at said destination device, and in response to said detecting, automatically destroying a received electronic information package.

A1

Claim 33 (Original): The method as claimed in Claim 28, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting a second or repeated attempted to play or display information package content, and in response to said detecting, automatically destroying a received electronic information package.

Claim 34 (Original): The method as claimed in Claim 30, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying, downloading, printing, and saving, received electronic information packages.

Claim 35 (Original): The method as claimed in Claim 30, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting a pressing of a key on a keyboard operable for said destination device.

Claim 36 (Original): The method as claimed in Claim 24, wherein said step of determining fulfillment of one or more certain conditions at said destination location includes the step of: identifying a user at said destination location for which access to these information packages is allowed.

Claim 37 (Currently Amended): The method as claimed in Claim ~~36~~ 24, wherein said enabling a sender of a communicated package to observe a user requesting access to content at said

A1

destination location ~~identifying step~~ includes implementing video camera device for generating video signals at said destination device for receipt by said sender, said sender receiving and displaying video signals at said sending device for identifying users attempting to read or play information package content at a destination device.

Claim 38 (Currently Amended): The method as claimed in Claim ~~37~~ 36, wherein said identifying step further includes:

enabling users to present a password to said method; and,

verifying a user's password prior to enabling access to said information package.

Claim 39 (Currently Amended): The method as claimed in Claim ~~37~~ 36, wherein said identifying step further includes authentificating said user by enabling users to present biometric data on/verification that include one or more of the following: biometrics, fingerprint, and voice data, said method including comparing input biometric data with predetermined biometric data corresponding to the intended recipient.

Claim 40 (Original): The method as claimed in Claim 24, wherein said step of determining fulfillment of one or more conditions at said destination location includes identifying an electronic system at said destination location for which access to these information packages is allowed.

Claim 41 (Currently Amended): A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for

A1

controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said method steps comprising:

determining fulfillment of one or more conditions at said destination location, said determining including enabling a sender of a communicated package to observe a user requesting access to content at said destination location and identify said user as a condition; and,

in response to determination of a fulfilled one or more certain conditions, enabling access to content provided in a communicated package.

Claim 42 (Original): The program storage device as claimed in Claim 41, further including the step of automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions.

Claim 43 (Original): The program storage device as claimed in Claim 42, wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals from receipt of an electronic package, said method further comprising the steps of:

determining elapsed time from receipt of an electronic information package; and,

generating a signal for initiating automatic destruction of the received electronic information package after said elapsed time interval.

Claim 44 (Original): The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more conditions at said destination device further comprises detecting an attempted performance of a forbidden operation at the destination location; and, in response to said detecting, automatically destroying a received electronic information package.

A1

Claim 45 (Original): The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: receiving a direct command signal from a sender at a sending device for initiating destruction of said electronic information package.

Claim 46 (Original): The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, and in response to said detecting, automatically destroying a received electronic information package.

Claim 47 (Original): The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting a second or repeated attempted to play or display information package content, and in response to said detecting, automatically destroying a received electronic information package.

Claim 48 (Original): The program storage device as claimed in Claim 43, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying, downloading, printing, and saving, received electronic information packages.

A1

Claim 49 (Original): The program storage device as claimed in Claim 43, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting a pressing of a key on a keyboard operable for said destination device.

Claim 50 (Original): The program storage device as claimed in Claim 43, wherein said step of determining fulfillment of one or more certain conditions at said destination location includes the step of: identifying a user at said destination location for which access to these information packages is allowed.

Claim 51 (Original): The program storage device as claimed in Claim 50, wherein said identifying step includes:

enabling users to present a password to said method; and,

verifying a user's password prior to enabling access to said information package.

Claim 52 (Original): The program storage device as claimed in Claim 50, wherein said identifying step includes authenticating said user by enabling users to present biometric data on/verification that include one or more of the following: biometrics, fingerprint, and voice data, said method including comparing input biometric data with predetermined biometric data corresponding to the intended recipient.